AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ❒ Original ❒ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Southern District of Georgia

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* ONE CELLPHONE WITH IMEI: 354214987835401, BELONGING TO APRIL EVALYN SHORT, CURRENTLY LOCATED AT FT. EISENHOWER	)	Case No. 1:23-mj-63

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Southern District of Georgia *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before December 21, 2023 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ❒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Brian K. Epps.

(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for ____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of ____.

Date and time issued: 12-7-2023, 2:30 pm

Brian K. Epps
Judge's signature

City and state: Augusta, Georgia

Brian K. Epps, U.S. Magistrate Judge
Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
1:23-mj-63	14 Dec 23, 9:35 am	

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Image of property in attachment A for items listed in attachment B.

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 14 Dec 23

Matthew B. Ehrhart

Executing officer's signature

Matthew B. Ehrhart, Special Agent

Printed name and title

ATTACHMENT A

Item to Be Searched

SUBJECT CELLPHONE: Blue Samsung cellphone: IMEI: 354214987835401 with a black Otter Box case belonging to SUBJECT. SUBJECT CELLPHONE is currently stored within the FEGA CID Office's Evidence Room, located at 321 Brainard Avenue, Fort Eisenhower, Georgia 30905.

ATTACHMENT B

Particular Things to be Seized

All records, including those stored digitally, pertaining violations 18 USC 1111(a):

1. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

   (a) evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

   (b) evidence of the attachment of other devices;

   (c) evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

   (d) evidence of the times the device was used;

   (e) passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

   (f) applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be

necessary to access the device or to conduct a forensic examination of it;

(g) records of or information about Internet Protocol addresses used by the device;

(h) records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

(i) As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

2. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (i.e Nintendo Switch's, Sony PlayStation's and Microsoft Xbox's); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives

intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

SEARCH PROCEDURE FOR DIGITAL DEVICE(S)

3. In searching digital devices (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

(a) Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.